

## **AFFIDAVIT IN SUPPORT A CRIMINAL COMPLAINT**

I, Peter J. Mauro, a Special Agent (SA) with the Federal Bureau of Investigation (hereinafter “FBI”), Cleveland Division, being duly sworn, depose and state as follows:

### **INTRODUCTION AND AGENT BACKGROUND**

1. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, the offenses enumerated in 18 U.S.C § 2516. I have been trained in advanced investigative techniques and have satisfied all requirements defined by the Federal Criminal Investigator Classification series established by the U.S. Office of Personnel Management.

2. I have been employed by the FBI as a Special Agent since August of 2009 and am currently assigned to the Cleveland division, Akron Resident Agency. I have been assigned to, and participated in, investigations in the area of general criminal matters, specializing in Crimes Against Children and crimes involving the internet. I have participated in all of the usual methods of investigation including, but not limited to, financial analysis, physical surveillance, service of subpoenas, cooperating witnesses, confidential human sources, telephone toll record analysis, interception of wire and cellular telephone communications, consensual monitoring, and the execution of search and arrest warrants. I have gained experience through training at the FBI Academy in Quantico, Virginia and everyday work relating to conducting these types of investigations. I am an FBI certified Computer Analysis Response Team (CART) Technician, and an FBI Digital Extraction Technician (DEXT). Prior to the FBI, I enlisted in the United States Air Force where I attained the rank of Staff Sergeant. I hold an associate’s degree in criminal justice, a bachelor’s degree in psychology, and a master’s degree in criminal justice.

3. Over the course of my employment as an FBI Special Agent I have conducted and participated in multiple criminal investigations that have resulted in arrests for violent criminal offenses involving children. These crimes resulted in subsequent convictions in Federal Courts.

4. This affidavit is being submitted for the limited purpose of establishing probable cause to believe that Rudolf A. Johnson (Johnson), date of birth December XX, 1978, has violated 18 U.S.C. § 2252A – Certain activities related to material constituting or containing child pornography, 18 U.S.C. § 2252(a)(2) - Receipt and distribution of visual depictions of minors engaged in sexually explicit conduct.

5. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents, Task Force Officers [TFO] and FBI Analysts, written reports about this and other investigations that I have received directly or indirectly, from other law enforcement agents, information gathered from the results of physical surveillance conducted by law enforcement agents, the service and execution of administrative subpoenas and federal search warrants, interviewing Johnson and his employer and IT clients, independent investigation and analysis by FBI agents/analysts, and my experience, training and background as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause for the requested complaint.

6. In or about February 2023 while running investigative queries in a law enforcement service<sup>1</sup> used to track Internet Protocol (IP) addresses suspected of trading Child Sexual Abuse Material

---

<sup>1</sup> It should be noted that the law enforcement service used herein does not provide the user with the actual CSAM media to review. It simply provides MD5 values of the suspected CSAM files, summaries of the files, and the file names along with technical data regarding when the files were transmitted to a specific IP address, and when that conduct occurred.

(CSAM) via an identified, peer-to-peer file sharing service, hereafter referred to a P2P, I observed IP 24.166.62.108 engaged in the receipt, possession, transportation, and distribution of files with matching MD5<sup>2</sup> values of known CSAM. The conduct occurred from on or about April 7, 2022 through on or about February 21, 2023.

7. On or about February 21, 2023 I identified IP address 24.166.62.108 actively participating on P2P receiving and sharing parts of files with MD5 values matching known CSAM. Specifically, from on or about April 7, 2022 through on or about February 21, 2023 IP address 24.166.62.108 received or transmitted approximately 86,069 files of interest, of which, approximately 12,775 files were determined to be severe files<sup>3</sup>.

8. For example, On or about February 21, 2023 at 04:19UTC, IP address 24.166.62.108 downloaded a series of CSAM videos via P2P. The original investigator that reviewed these files described them as, "Prepubescent females engaged in sex acts." A review of the file names of this batch of CSAM included titles such as, "Damita - young south American girl.mpeg", "Passionate young lovers.mpg", "schoolgirl VERY good.mpg", "Cute Preteen learning new things.mpg", and "Teen Daughter raped by Daddy."

9. On or about February 21, 2023 at 03:23UTC, IP address 24.166.62.108 downloaded a series of CSAM videos via P2P. One such video during this download session is identified as MD5: A5AC651C793624B0B583EA7D8C32545F. The video is described as, A video compilation of a prepubescent girl aged three to five years old. The girl is observed reclined on her back with her legs in

---

The descriptions are law enforcement officer descriptions of CSAM that share the same MD5 value as those received, downloaded, and shared by 24.166.62.108 on P2P.

<sup>2</sup> MD5 is a nationally recognized file verification and authentication protocol used by the government and businesses to intercept and identify CSAM and to substantially compare like-files.

<sup>3</sup> Files of interest can be used by the law enforcement service to describe files that are child exploitative, age difficult, computer generated, or do not rise to the level of illegal, while severe files are described as CSAM.

the air exposing her vulva and anus. The girl masturbates for the camera inserting her fingers into her vagina. The camera focuses closely on the girl's genitals while she masturbates. An adult hand digitally penetrates the girl. Then, an adult male with an erect penis vaginally rapes the girl with his penis. This video is 48 minutes in length.

10. Thousands of other instances of file transmission matching known MD5 values occurred either to or from IP address 24.166.62.108; the described herein are a small sample of the greater available evidence. Geolocation information indicates that the IP address is located in the Akron, Ohio area.

11. On or about February 25, 2023, I requested the service of an administrative subpoena on Charter Communications for the subscriber of IP address 24.166.62.108 for the time period of inclusive conduct.

12. On or about February 27, 2023 Charter Communications responded and indicated that IP address 24.166.62.108 was subscribed to Rudolf Johnson at XXX Carnegie Avenue, Apartment C7, Akron, Ohio 44314-1142 from on or about April 6, 2022 through February 22, 2023. Charter Communications also indicated that the billing and service address were both listed as 685 Carnegie Avenue, Apartment C7, Akron, Ohio 44314-1142, identified as The Premises.

13. On or about February 28, 2023, Detective Dan Maher, #6128, of the Circleville Police Department, and a task force officer assigned to the Ohio Internet Crimes Against Children Task Force provided me CSAM evidence obtained from IP address 24.166.62.108 via P2P. Detective Maher utilized a law enforcement tool on P2P to directly connect his law enforcement computer and conduct a single-source download of offered CSAM files directly from IP address 24.166.62.108, and only that IP address.

14. The evidence provided by Detective Maher contained approximately 420 files of CSAM. Of the 420 files, 240 were images and 180 were videos. The download also contained 1,450 files of Child Exploitation Material (CEM) (CEM is described as either "age difficult" media, or exploitive media that may not meet the definition of lewd or lascivious). The date of conduct occurred from on or about April 7, 2022 through on or about February 21, 2023.

15. The media from Detective Maher is described in part below:

16. A three minute, 33 second color video titled, "NewSugar07.avi" depicts an approximately two-year-old female toddler. The toddler is laying on a bed on her back naked from the waist down. An adult male hand is observed pulling the girl's labia apart exposing her vagina for the camera. The man then digitally penetrates the girl's vagina. Then, an erect adult male penis can be seen. The man then vaginally rapes the child with his penis. The girl is then forced to perform fellatio on the man. The video concludes with the man ejaculating on the girl's face.

17. A one minute, 21 second color video titled, "pthc cum over babygirl 5yo.mpg" depicts an approximately one-year-old baby girl. The baby is laying on a bed completely naked. An adult male with an erect penis is vaginally raping the girl. The video pans up and the baby is playing with a teething toy while the man engages the girl. The video ends with the man ejaculating on the face and bare chest of the little girl. I know that "pthc" mean "pre-teen hard core" in the world of CSAM.

18. A 48 second color video titled, "300.avi" depicts an approximately seven-year-old girl naked except for a choker leash around her neck. the girl is on her hands and knees manually masturbating and performing fellatio on a barn animal with an erect penis. Due to the camera angle, it is uncertain what kind of animal is in the video, but is likely a sheep or goat.

19. A color image titled, "000068.jpg" depicts an approximately six-year-old girl with her skirt pulled up around her waist exposing her buttocks. The girl's hands are bound behind her back with rope. An adult male with an erect penis is observed anally raping the girl.

20. A 42 second color video titled, "papa t babyj 5yr assfuck(2)(2)(2)(2).avi" depicts an approximately five-year-old girl laying naked on her back with her legs spread exhibiting her vulva. An adult male with an erect penis is observed anally raping the girl for the duration of the video.

21. The remaining files are similar in likeness and kind to those described herein.

22. A search of the Ohio Bureau of Motor Vehicles revealed that Johnson has two passenger vehicles registered to his name at The Premises, and that he is the sole registrar on both vehicles.

23. A search of open-source internet revealed a LinkedIn profile in the name of Rudolf Johnson. The profile lists Johnson as located in Akron, Ohio, a former attendee of the University of Akron, and was a computer technician. The profile has a color image of Johnson, that matches Johnson's Ohio BMV image.

24. FBI physical surveillance in March, 2023 has confirmed that Johnson resides at XXX Carnegie Avenue Apartment C7, Akron, Ohio, and has indicated that no other residence likely reside there with Johnson. FBI surveillance has also indicated that Johnson works in the IT department of Summa Health in Akron, Ohio.

25. On or about April 6, 2023 Akron FBI executed a federal search warrant on Johnson's residence. Contemporaneous to the execution of the search warrant, I conducted a surreptitiously recorded interviewed of Johnson:

26. Johnson was informed that the interview was voluntary. Johnson was reminded of that fact midway through the interview. Johnson indicated that he has resided at his residence for

approximately 10 years. Johnson stated that he resides alone and is employed as an IT customer support person for Summa Health system. Johnson indicated that he holds a degree in Economics.

27. Johnson was informed that the interviewers were interested in suspicious internet traffic that was entering and exiting the internet network of his apartment. Johnson said that he had an idea that the Agent and Task Force Officer were speaking to him about Torrents. Johnson admitted to using P2P and other torrents for a very long time, estimating that it has been going on since at least when he was in college. Johnson stated that he downloads, saves, and shares child pornography, and stated that he understands what child pornography is. Johnson described child pornography as pornography that depicts children engaged in sex acts. Johnson agreed that the child pornography that he seeks out and masturbates to depicts pre-pubescent children under the age of 12.

28. Johnson stated that he actively seeks out child pornography on P2P and that he shares it with others. Johnson detailed specifically how he seeks child pornography on P2P by searching terms like “teen” “young” “pre-teen” and “amateur”. Johnson was directly asked if he searches “PTHC or pre-teen hardcore” to which he declined. However, Johnson indicated that there is no distinction between the two and the results they produce are similar. Johnson discussed how he distributes and shares child pornography by allowing access to child pornography saved on his hard drive, and limiting the bandwidth of that sharing, indicating an intimate knowledge of the workings of P2P. Johnson was directly questioned by the interviewers:

- “How frequently do you share images and videos under 12?” To which Johnson replied, “Unfortunately, they are getting distributed from my computer at the moment.”

29. Johnson described the types of pornography he consumes and views. Johnson stated that he views pornography of pubescent teenage girls, as well as prepubescent children. Johnson admitted to downloading, possessing, viewing and sharing toddler-aged child pornography, child pornography that involved bondage, as well as child pornography that depicts bestiality involving children with animals. Johnson admitted to masturbating and self-pleasure while viewing child pornography. Johnson admitted to viewing child pornography on an approximate weekly basis, last viewing it the previous week from the interview.

30. Johnson described his hardware setup; Johnson stated that he has a desktop computer running Windows with 32GB of RAM, and a two-terabyte hard drive. Johnson admitted that all of the child pornography that he possesses exists on that computer hard drive. Johnson stated he built that computer himself and was his. Johnson denied using any forms of encryption or encrypted containers.

31. Johnson stated that he conducted IT work on the side, outside of Summa Health for private companies. Johnson stated that some of the hardware present at his residence was that owned by outside clients that he contracts for.

32. Johnson denied any hands-on offenses. Johnson stated that he presents himself with a level of decorum in public, and that would preclude him from any hands-on offenses. Johnson admitted knowing that his conduct looking at child pornography is wrong.

33. The federal search warrant conducted on Johnson's residence revealed the desktop computer Johnson referenced in his interview. A cursory review on-scene by a CART employee revealed a folder titled, "8 yo daddy's little girl". Inside that folder were four video files consistent with CSAM. The desktop computer and other computer peripherals were seized from his residence.

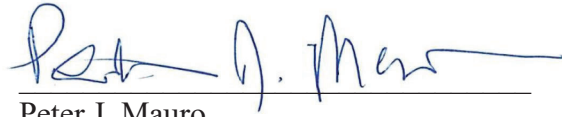


34. On or about April 12, 2023, at approximately 8:00am, while conducting an unrelated CSAM investigation, I interviewed the owner of an Akron business identified hereafter as CW1. CW1 was informed that an IP address associated with her company had downloaded approximately 60,000 files of CSAM since May, 2022 and most recently at or about 7:22am on the date of the interview. On the date of the interview, April 12, 2023 more than 400 files of CSAM were downloaded by CW1's company's IP address at or about 7:22am. CW1 consented to a search of all of the computers at her business. During the investigation, it was learned that CW1 employed an outside computer IT contractor to setup and manage her company's computer network. CW1 volunteered that the company used Johnson as the sole IT contractor. Johnson set up, managed, and maintained CW1's computer network and has for years. CW1 indicated that Johnson often logs in remotely and manages their network from home. CW1 stated that Johnson also takes and performs maintenance of computers from CW1's company at his home, before returning them a few days later.

35. A review of the file names included in the approximately 400 files downloaded on or about April 12, 2023 via CW1's company's IP address are consistent with filenames of files downloaded by Johnson on his home computer. These titles include titles such as, "Pthc Girl Man – Dark Secret 5Yo Child Abuse 2.mpg" "New Pedo PTHC 6yo 2011 friend3.avi".

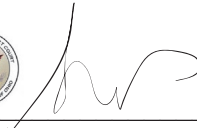

### **CONCLUSION**

36. Based on the above information, probable cause exists that Rudolf A. Johnson violated has violated 18 U.S.C. § 2252A – Certain activities related to material constituting or containing child pornography, 18 U.S.C. § 2252(a)(2) - Receipt and distribution of visual depictions of minors engaged in sexually explicit conduct.



Peter J. Mauro,  
Special Agent  
Federal Bureau of Investigation

Sworn to via telephone after submission  
by reliable electronic means.  
Fed. R. Crim. P. 3, 4(d), and 4.1,  
on this 12<sup>th</sup> day of April, 2023



AMANDA M. KNAPP  
UNITED STATES MAGISTRATE JUDGE